RESEARCH GRANT PROPOSAL

For

WASHINGTON STATE FERRIES

WIRELESS CONNECTION PROJECT

To

Ms. Charlene M. Wilder
Transportation Management Specialist

Federal Transit Administration
Office of Mobility Innovation, TRI-10
400 7th Street, SW, Rm 9402
Washington, D.C. 20590

1.0 Introduction

1.1   Purpose
The Purpose of this research and development project is to study the feasibility of the Washington State Ferries using 802.11 Wi-Fi data network on board the ferries to develop a Floating Area Network (FAN). The title of the project is the Washington State Ferries (WSF) Wireless Connection Project.

1.2   Scope
The scope of this document, Grant Proposal, is to describe the project more fully, to address questions, to show cost information, to tie deliverables to each task, and show a list of formal contract deliverables.

1.3   General Information

Client: Washington State Ferries

Location: 2911 Second Ave
                       Seattle, WA 98121-1012

Services: Provides Vehicle and Passenger Transportation across the Puget Sound.

Customer/Market: Puget Sound Region and the State of Washington

WSF Contact: Mr. John Daane
                       (206) 515-3802
                       daanejo@wsdot.wa.gov

Consultant: Mobilisa, Inc.

Location: 2023 E Sims Way #346
                       Port Townsend, WA 98368

Consultant Contact: Dr. Nelson Ludlow
                       (360) 344-3233
                       nelson.ludlow@mobilisa.com
                       www.mobilisa.com

Proposed System: Washington State Ferries Wireless Connection Project (WSFWCP). This project will evaluate the feasibility of installing an 802.11 data network on board the Washington State Ferries.

2.0　Technical Objectives

2.1　General Objectives

2.1.1　Wireless for Passengers
Passengers will be able to access the Internet both while waiting for the boat in parking areas and terminals, as well as while onboard. During peak traffic times, passengers in vehicles may have to wait hours and then spend an additional 30-60 minutes onboard. Passengers can make use of the network to check email, pay bills, surf the net, or simply to improve their travel experience.

2.1.2　Wireless for Services Onboard
The galley will be able to accept credit and debit cards for the first time. ATM machines, which had previously made use of a spotty cellular connection, will be able to make transactions across the network. Clearly this service requires security to handle financial information. GPS reporting and other onboard services, such as Smart Card replenishment/reload may also be able to be provided.

2.1.3　Backup Wireless for Crew
If existing radio or wireless communication systems fail, the crew could use this system for safety alerts, weather updates, and even Voice Over IP (digitized voice over the internet), for those WSF onboard computers/IP Phones having wireless modems installed.

2.2　Functional Objectives

2.2.1　Continuous Coverage
It is critical that connectivity run the full length of the route. The benefit becomes greatly diminished if there are dead zones in the coverage area. Transactions could be cut-off halfway, crew augmentations would not be dependable, and customers accessing the Internet would undoubtedly be upset.

2.2.2　Security
Credit and Debit card information will need to be kept private. Passenger connection will not use encryption methodology as this methodology uses a secret password on both ends of transmission. The goal of the passenger network is to have many passengers use the same system. A so-called "secret" encryption key would be of little value if it were shared with the public using the net. Therefore, the ability for a passenger to use secure socket layer (SSL) and virtual private Network (VPN) technology is required.

2.2.3　Non-interference with Existing Communication Systems

There are communications taking place on board the ferries in the same spectrum in which 802.11B operates. Interference between competing systems is unacceptable. Location of antennas and channel selection is important to prevent interference with existing communication systems.

2.3   Problems to be Addressed

2.3.1   Limited Range
The nature of the unlicensed spectrum and the low-wattage makes the range of antennas and access points a limiting factor. Range can be extended by using certain types of antennas and focusing the signal.

2.3.2   Moving Ships
The ferries will be moving and do not follow exact routes. Further, the routes are not necessarily straight, and the auto/passenger vessels must make turns to navigate into the terminals and to avoid other sea traffic. This prevents a fixed directional antenna onboard a vessel. Other techniques must be used.

2.3.3   Dirty Power
The power that is generated on the ferries is not the same as the power on land. The power system on the ferries is susceptible to power surges, which is incredibly damaging to computers and electronic circuitry.

2.3.4   Changing Vessels on Routes
Several vessels serve as system wide back-ups, so changing a vessel to serve a different route is normal, and should be planned for. Cost considerations of equipment need to be addressed in conjunction with this requirement, as certain routes may require more expensive equipment. This cost trade-off analysis will be part of the system architecture.

3.0 Technical Background

3.1 802.11 Wi-Fi for Data Communications

802.11 is an IEEE standard for wireless communications. It is rapidly growing in popularity and is also known as Wi-Fi (Wireless Fidelity). It makes use of existing technology to provide a wireless internet connection over the unlicensed Industrial Scientific Medical (ISM) radio spectrum. Wi-Fi can provide an inexpensive internet connection with high speed bandwidth for data.

3.2 Different 802.11 Standards

There are several 802.11 wireless modes. Briefly, let's look at six different wireless modes, and their strengths and disadvantages:
- 802.11 RF Frequency Hopping
- 802.11 RF Direct Sequence
- 802.11 Infrared
- 802.11b RF
- 802.11a RF
- 802.11g RF

The standard 802.11 was written in 1997. There were several manufactures of these products, and our team has used most every product on the market. They provided 1 and 2 Mbps data transfer data speeds and three different transmission methods: RF Frequency Hopping, RF Direct Sequence, and Infrared. The two RF modes operate in the unlicensed Industrial, Scientific, Medical (ISM) frequency spectrum. Infrared operates in the light spectrum and does not require a license.

The frequency hopping spread spectrum (FHSS) method was borrowed from the military, and used multiple frequencies to jump between, essentially transmitting each bit on a different frequency in a pre-set pattern. The problem for this mode is that it did not provide any real security, as all the systems had to know the frequency hopping pattern to be able to transmit and receive, unlike the military system where the pattern was secret,. However, it did provide for a spread-spectrum capability which was more resistant to interference.

The Direct Sequence Spread Spectrum (DSSS) method is the method used in the newer standard of 802.11b. Also using spread spectrum, this method uses a spreading code algorithm to replicate each data bit with multiple transmissions. It is somewhat more prone to interference than FHSS, and has the ability to work with different channels to lessen interference between wireless systems. Notable is that the FHSS and DSSS systems will not work with each other.

Both the FHSS and DSSS have similar ranges that vary with manufacturers. Typically access points transmit at a power of 500 milliwatts, and can attain ranges of 500m in open space with an Omni-directional antenna, and much

further with a Yagi antenna. In closed spaces, particularly inside metal structures, they attenuate significantly. Further, *multipath delays* can be caused by "echoes" of the signal bouncing off the metal wall taking different paths to reach the access point at different times.

Infrared is another wireless means. Governed by 802.11, it also operates in the 1 and 2 Mbps, with new Fast IR operating at 4Mbps. It is narrow beam IR, which is different than the remote control for a television, which is wide beam and transfers at a much slower speed. IR devices are becoming more ubiquitous and are in essentially all laptop and handheld computers. IR's biggest limitation is distance. Typically ranges are all under 1 meter, and we find in practice actually closer to 30cm. Another disadvantage is that the user has to hold and point their device directly at the access point. Further, it cannot penetrate walls. Therefore, this is an unlikely method for wireless on metal ships.

The earlier 802.11 products were not generally accepted. However, 802.11b products became very popular and are now used everywhere in government and business.

The three biggest advantages are the increase in data rates to 11Mbps; they are cheap (many low-end commercial systems are under $100); and they are well known (easier to find personnel who understand the system to maintain it, et cetera). They have similar ranges to 802.11 systems as would be expected, however the data transfer speed changes with distance—the closer the transceiver is to the access point the faster the transfer rate. Typical ranges are 0-59 feet for 11Mbps, 60-119 feet for 5.5Mbps, and over 120 feet for 1 Mbps.

Wireless Access Points

The 802.11a standard has provided several products on the market in the last few months. It operates in the 5 Ghz band and can achieve speeds of 54Mbps. This is good for required high bandwidth at short distances, such   as video links in a command and control center. However, it has even worse degradation of speed at increased distances!

The latest 802.11g standard is essentially 802.11b standard at the faster speeds of 802.11a, which are 54 Mbps. Most importantly, it is downwardly compatible (which is a first for wireless LAN standards). 802.11g provides the greatest range of speed for price with the greatest accessibility by the typical ferry passenger.

3.3   Coverage and Overlapping Issues

Site Surveys will be conducted onboard the auto/passenger vessels to ensure we can provide adequate coverage to passengers and services. Mobilisa conducted a site survey onboard the Washington State Ferry MV Tillikum.   They tested 802.11b, 802.11a, and 802.g-- both on the passenger and car decks.

802.11 Access Points Evaluation aboard MV Tillikum.

To achieve adequate coverage, typically overlap is required or encouraged. Often the placement of two access points (AP) on opposite sides of the room may achieve better coverage than a single access point placed in the center of the room. The goal is that any areas that are in a shadow caused by some blockage will be covered by the placement of the second access point.
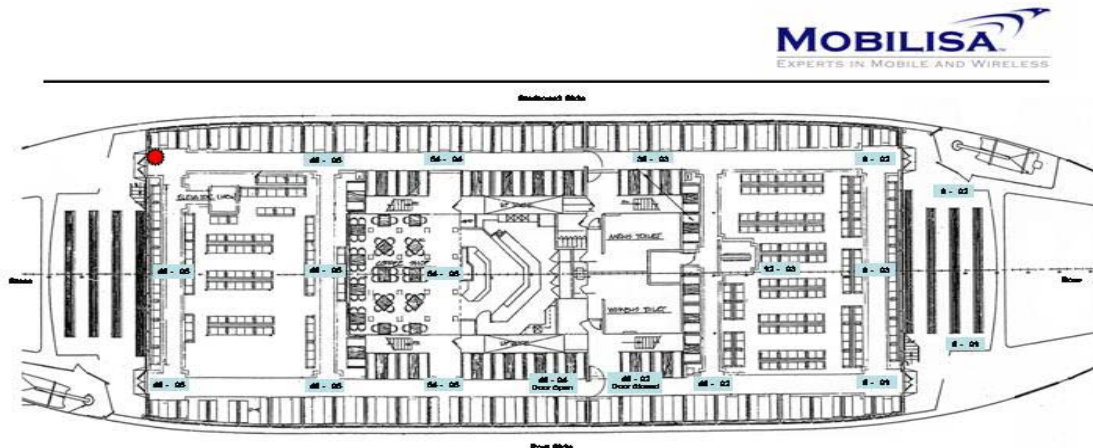
Ferry Passenger Deck
Selected Readings with "G" Access Point

As an example, the above diagram shows signal readings that were recorded for 802.11g onboard the MV Tillikum on the passenger deck.

3.4   Bandwidth and Use Requirements

Bandwidth or data transfer rates are directly related to distance of transceiver from the access point. Typically the higher the frequency of the system, the quicker the bandwidth drops based upon distance. At the 2.45 Ghz range, you may cut your transfer rate to 10% by moving just 60 feet! (Based upon 0-59 feet for 11Mbps, 60-119 feet for 5.5Mbps, and 1Mbps after that).

3.5   Wireless Security

The UC Berkeley paper "Intercepting Mobile Communications – The Insecurity of 802.11" described two guys in a van eavesdropping on wireless LANs from several Silicon Valley companies. Most of these companies had never set their ESSID to anything other than the factory preset (the ESSID allows different WLANs to operate within the same space), and they did not turn on the Wireless Encryption Protocol (WEP). A study of over a dozen access points showed that all of the factory presets are set to *WEP-Off.*

Mobilisa conducted a similar survey in the heart of Washington DC. Their wireless engineers were working at NASA HQ to improve wireless security. Using "war-driving" techniques, they discovered over 50 access points at various government agencies, of which approximately 85% did not have encryption turned on.

There are several types of WEP: WEP 64 (actually 40-bit), Super WEP 128 (actually 104-bit), and WEP 156 (actually 132-bit). The 40-bit WEP is the most commonly used. Examples of equipment encryption methods are the Lucent ORINOCO Gold card and Cisco Aironet card which are capable of 104-bit using RSA RC4 encryption. NetGear 802.11a uses 132-bit encryption.

Secure Socket Layer (SSL) and data encryption is required for secure data transactions such as debit and credit card. Washington State Ferries is the largest user of debit/credit card transactions in the State of Washington.

Passenger use cannot make use of WEP. WEP relies on the concept of a secret password. For public use, the concept of secret password cannot work. In a public use environment, typically WEP is turned off. Rather, another method of access and control is used.

We will investigate access and control servers that require a password and are recorded to username and MAC address for validation, and possible payment collection per passenger. Software will be developed to provide web pages for access information and instructions of use.

The WSF system needs to be able to allow personal use of a Virtual Private Network (VPN) through the wireless network. That will allow users to protect their own data if they wish.

4.0 Proposed Research and Development

4.1 Requirements Analysis

Determine the specific requirements for the wireless connection project. This includes determination of specific travel routes to be covered, required wireless bandwidth, and coverage aboard the ferries, terminals or parking areas. A determination of data requirements and security concerns for any crew or onboard services (e.g. restaurants, ATM, etc.) will be described. Determination of customer access and control requirements and software needs will also be determined and documented.

A formal Systems Requirements Specification (SRS) will be developed in accordance with CDRL A0014.

4.2 Business Case Study

A formal study will be conducted to review business case options of how to implement wireless services for WSF customers. Type of services, length of use, time of use, internet services used, and likely equipment used by customers will be reviewed. The study will also evaluate other wireless ISP models, and discuss potential revenues generated from passenger use. A survey of WSF riders will be conducted and incorporate previous survey information.

A Business Case Study document will be developed in accordance with CDRL A003.

4.3 Develop Engineering Design

Using the Requirements Document, a formal design of the wireless connection system will be developed and documented. Major areas of the Engineering Design include:
- Shore to Vessel Back-Haul
- Testing of Backhaul Equipment
- Ship to Customer Distribution
- Security
- Customer Access and Control
- Software Design
- Access Point Placement
- Load Analysis
- Review Equipment Options

Shore to Vessel Backhaul will include a review of selected routes, terminals, and likely antenna placement, and a review of Line Of Sight (LOS) requirements. Some experimental testing of various backhaul equipment and access/control/security equipment will be live tested to determine the best combination of equipment for implementation.

Testing of backhaul equipment and limited onboard vessel testing will be conducted on the Port Townsend – Keystone run. This run is ideal as it a relative short distance between terminals, is a small boat with less passengers than the Jumbo class ferries, and near the contractor's offices in Port Townsend. It is expected the beta equipment would be aboard one ferry, which is the main ferry used for winter and summer runs.

An evaluation of Back-haul equipment will be described in a technical report in accordance with CDRL A005. Recommended locations of Antenna locations will be delivered in a antenna placement plan in accordance to CDRL A013.

A ship to customer distribution architecture will be designed. It will take into account estimated Load Analysis, Customer Access and Control, and Security.

A Systems Architecture and Design Document will be presented in accordance with CDRL A016, and if necessary an Interface Requirements Specification in accordance with CDRL A015.

The software to implement the access and control of passengers onto the system will be implemented via a web based approach, and use username, password, and possible hardware verification such as MAC Address. The web pages will control access, explain how to purchase or gain access, and provide instructions. The web pages should also have some standard WSF information, such as schedule and announcements of service changes.

A software design document will be presented in accordance with CDRL A017.

Necessary site surveys, and use of any automated Wireless LAN Design tools to aid in the placement of access points aboard the auto/passenger vessels will be conducted. Similar classes of vessels may not require a complete site survey. Site surveys of the installed terminals and parking areas will also be conducted.

The results of the site surveys will be delivered as a wireless coverage diagram in accordance with CDRL A012.

A review of electrical power access and installation method will be shown in an engineering drawing(s) showing the equipment location and any modifications to bulkheads.

An engineering drawing showing the equipment installation will be delivered in accordance with CDRL A006.

A test of the installed access points will be tested for use and capability. Further, simulation tests will be conducted for load analysis.

The Systems Test Plan, CDRL A018; Systems Test Description, CDRL A019; and CDRL A020, Systems Test Report will be provided.

A list of equipment recommendations and implementation will be delivered in accordance with CDRL A022.

A formal presentation summarizing all the findings and design information will be delivered as CDRL A010 for the Agenda and CDRL A011 for the presentation materials.

4.4 Implement and Test with Passengers on Selected Vessels and Terminals

Implement the wireless system which will require installing wireless access points aboard the vessels and in the terminals, backhaul communications between ship and shore, and coordination of wired service provided by a carrier. A complete integration of the system (including computer hardware, software, off-site servers, and wireless antenna systems and routers) will be set up to provide wireless services for the selected vessels and terminals.

Approximately nine auto/passenger vessels (in addition to the one beta test vessel on the Port Townsend – Keystone run mentioned in section 4.3) will be required to be outfitted with equipment to cover the selected routes of:
-- Seattle – Bainbridge Island;
-- Seattle – Bremerton;
-- Edmonds – Kingston.

A live demonstration of the system will be offered in accordance to CDRL A002.

Evaluation with a limited passenger use, and system improvements will be made based on the internal evaluation. Passenger evaluation data will be collected and delivered in a formal report of findings.

The passenger evaluation report will be delivered in accordance of CDRL A021.

4.5   Evaluate System

An independent review will be conducted by a third-party consistent with FTA requirements. This task involves an independent review of the design and test implementation of a WLAN system deployed on Washington State Ferries.

The first aspect of the system evaluation will validate the network design of wireless access coverage and capacity of the deployed WLAN as envisioned per the design. Additionally, this aspect of system evaluation will analyze the interference between multiple coverage areas. This validation will cover the design areas of:

- Access Point Placement (coverage + interference)
- Antenna Systems
- Load Analysis (capacity)

The second aspect of system evaluation will validate the ease of access for passenger subscribers and ensure that access to the WLAN is limited to those who have appropriate authorization. This aspect of system evaluation will cover the design areas of:

- Security
- Customer access and control

The third aspect of system evaluation will validate the ability of the WLAN deployed on the vessel to provide a "pipe" to the internet as well as WSF intranet. This aspect of the system validation will cover the design areas of:

- Vessel to shore backhaul
- Testing of backhaul equipment
- Continuous and uninterrupted service availability during vessel travel

The third-party will provide a Test Plan, CDRL A008; Test Description, CDRL A009; and CDRL A010, a formal Test/Inspection Report of findings will be provided.

4.6   Provide System Support

The system will be maintained via network engineer support, coordination with wired carrier service providers, and limited help desk support to customers. The capability to review network status and capabilities, and passenger use statistics will be developed.

Improvements and upgrades to the system may be suggested by WSF and implemented by the Contractor.

The amount of service provided under Task 6 will be determined on a Time and Materials (T&M) basis.

4.7   Monthly Progress Reports

The consultant will provide to WSF and the Government a monthly report of progress to state work conducted, accomplishments, issues noted, and expenditures of funds.

A monthly status report will be delivered in accordance to CDRL A001.

5.0   Work Plan

5.1   Statement of Work

Performance of this contract by the Contractor shall be in accordance with the detailed obligations to which the Contractor committed itself in the Contractor's proposal by Mobilisa in accordance with the Grant Proposal entitled "Washington State Ferries Wireless Connection Project," dated 5 May 2003, submitted in response to a verbal request by Ms Charlene Wilder, Federal Transit Administration FTA/TRI-10, Office of Mobility Innovation. The technical volume of the Contractor's proposal is incorporated by reference and hereby made subject to the provisions of this contract, as if included in full text herein.

Periodic progress reports, requirements documents, functional specifications, design document, test plan, inspection reports, and any other evidence of contract deliverables shall be delivered in accordance with the Contract Data Requirements List, in section 5.2. All reports delivered by the Contractor to the Government under this contract shall prominently show on the cover of the report the following information:

(a)   Name and business address of contractor.
(b)   Contract Number.
(c)   Technical Point of Contact (TPOC) or Contacting Officer Representative (COR), name, office symbol and phone number.
(d)   Grantee (Washington State Ferries)
(e)   Contracting Office: Washington State Ferries
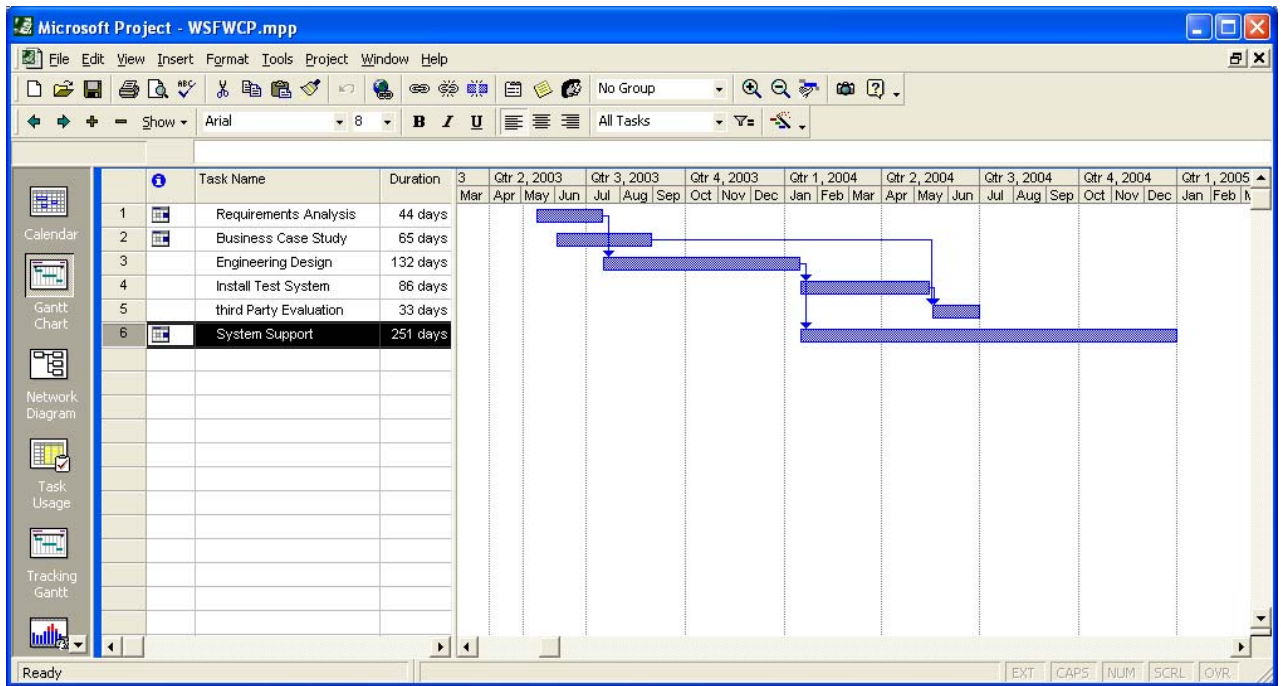   *2911 2ⁿᵈ Avenue*
            Seattle, WA 98121-1012

5.2　　Contract Data Requirements List (CDRL)

A001　CONTRACTOR'S PROGRESS, STATUS & MANAGEMENT REPORT

A002　SYSTEMS DEMONSTRATION

A003　BUSINESS CASE STUDY

A004　SYSTEM DESIGN ANALYSIS REPORT

A005　SCIENTIFIC AND TECHNICAL REPORTS

A006　PRODUCT DRAWINGS AND ASSOCIATED LIST

A007　THIRD PARTY TEST PLAN

A008　THIRD PARTY TEST PROCEDURE

A009　THIRD PARTY TEST/INSPECTION REPORT

A010　CONFERENCE/MEETING AGENDA

A011　PRESENTATION MATERIAL

A012　WIRELESS COVERAGE DIAGRAM

A013　ANTENNA PLACEMENT PLAN

A014　SYSTEM REQUIREMENTS SPECIFICATION (SRS)

A015　INTERFACE REQUIREMENTS SPECIFICATION (IRS)

A016　SYSTEMS ARCHITECTURE AND DESIGN DOCUMENT

A017　SOFTWARE DESIGN DESCRIPTION (SDD)

A018　SYSTEMS TEST PLAN (STP)

A019　SYSTEMS TEST DESCRIPTION (STD)

A020　SYSTEMS TEST REPORT (STR)

A021　PASSENGER EVALUATION REPORT

A022　RECOMMENDED EQUIPMENT LIST

5.3   Schedule

Task	Start	Finish
1) Conduct requirements analysis	15 May 03	15 July 03
2) Develop business case study	02 Jun 03	29 Aug 03
3) Develop engineering design	16 July 03	15 Jan 04
4) Implement test system on selected vessels and terminals	16 Jan 04	15 May 04
5) Evaluate system	16 May 04	30 Jun 04
6) Provide system support	16 Jan 04	31 Dec 04
Project Complete		

*Assumes a contract start date of 15 May 2003.   Finish dates may be appropriately changed as days after contract award.

5.4   Overall Project Brief Information
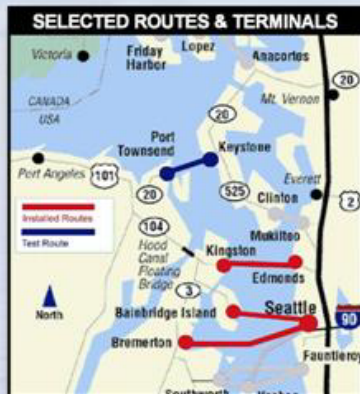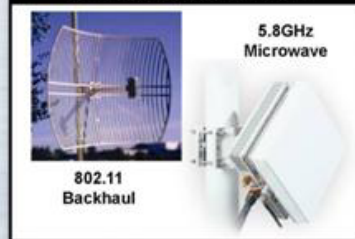
6.0   Related Work by Consultant (Mobilisa, Inc.)

Mobilisa, Inc. is a leader in 802.11 wireless aboard ships. They have vast experience in site surveys, wireless security, wireless equipment aboard   land-based structures as well as passenger ships and US Naval vessels.

Site Surveys: Mobilisa wireless engineers have been involved in numerous wireless site surveys for structures on land, as well as ships.   These structures include hotels, restaurants, business offices, passenger ferry and US Naval combat ships. This experience gives Mobilisa knowledge of what will work and what won't work, as well as complete understanding of the operations required to conduct a professional and safe site survey, particularly in the afloat environment.

Wireless Security Analysis: Mobilisa has conducted several wireless security analyses for customers including NASA HQ, Army Corps of Engineers, and the Washington State Ferry System.

Each particular analysis varies by customer requirements. As an example of services provided, Mobilisa conducted a detailed study of NASA headquarters' wireless computing systems.   Mobilisa completed detailed site surveys, found all radiating devices, determined current system settings, made recommendations on how to secure the system, and demonstrated how to crack WEP encryption. Three methods of cracking WEP were demonstrated, including one that is proprietary to Mobilisa. We used a host of tools, several of which are hacker tools, to fully evaluate the system.   Further we reviewed known wireless hacker sites to find previous penetrations of government systems.

Wireless LAN Design Tools: Mobilisa recently won a Small Business Innovative Research (SBIR) grant from the US Navy's Smartship Program. Under this contract, Mobilisa engineered the first phase of an expert system that can quickly design an affordable Wireless LAN that includes combinations of wired, wireless RF, wireless IR, and each evolving standard. The expert system uses 3-D space coordinates (i.e. blueprint info) as input, and produces optimal location for wireless access points and type of access point, wireless mode, and end-user transceiver requirements.

Shipboard Wireless LAN experience: Shipboard wireless is an interesting environment because the 802.11 signal does not travel well through steel and other metals. It also bounces off the surfaces causing a "multi-path" interference problem.   Mobilisa understands the wireless shipboard environment. Mobilisa has tested three separate 802.11 wireless systems aboard a passenger ferry, as well as placed numerous wireless systems aboard US Navy ships, including the Spruance-class Destroyer, USS David Ray.

Screen Shot of Mobilisa's Wireless LAN Design Tool called AIRCHITECT

Mobilisa Crew with Wireless Test Equipment aboard Navy Destroyer

7.0 Government Furnished Property/Material

The Washington State Ferries (WSF) will provide program management by Mr. John Daane. Mr. Jim Long, Director of Information Technology for WSF, will supervise Mr. Daane.

Access to auto/passenger vessels, terminals, antenna farms and towers, and parking areas, and when necessary, escort of contractor personnel is provided by WSF. The consultant contractor must coordinate all onsite visits and work periods with the WSF Program Manager.

Data items, drawings, computer data files, or blueprints that are required for the contractor to properly place antennas, wires, and access points will be provided to the consultant. WSF shall provide consultation on location of wiring systems, and when necessary, professional engineering services will be provided by WSF to ensure compliance with regulations.

WSF may provide the contractor with any necessary safety briefings.

Other WSF administrative functions of accounts receivable, accounts payable, contracts, legal, communications, engineering will support the successful completion of this project.

WSF will waive the travel fees of Mobilisa personnel onboard the ferry, while in conjunction with the engineering, installation, and support of this project.

It is anticipated that WSF will purchase the majority of the equipment required for the installation. This should provide WSF with the best purchase price of equipment. Equipment under the value of $10,000 may be purchased by the consultant contractor upon the written approval by WSF Program Manager, and equipment under the value of $1,000 upon the verbal approval of the WSF Program Manager.

8.0 Place of Performance and Travel

Place of Performance. Work under this task order is to be primarily performed at the contractor facility in Port Townsend, WA; at the seven WSF terminal locations (Coleman Dock/Seattle, Bainbridge Island, Bremerton, Edmonds, Kingston, Port Townsend, and Keystone), the Eagle Harbor Maintenance Facility, and aboard the necessary WSF auto/passenger vessels. A small percentage of the work may be performed at the computer facilities of WSF.

Local area travel by the contractor is required to the Washington State Ferry offices in Seattle, the seven WSF terminal facilities listed above, Eagle Harbor maintenance facility, aboard WSF auto/passenger vessels, and other locations within the Puget Sound that are required to complete this project.

Some minimal travel by WSF Personnel and Contractor to Washington DC, FTA offices may be required.

9.0 Security

9.1   Security

Security clearances are not required.

9.2   Safeguarding

The contractor shall provide safeguarding procedures for all data provided by WSF in accordance with their requirements. This is particularly important for all computer security interfaces.

10.0 Safety Equipment

10.1   Safety Equipment

Contractor and WSF will both use required safety equipment to include hard hats, protective eye wear, noise abatement devices or safety equipment in accordance with OSHA standards.

11.0 Inspection

11.1   Inspection and Acceptance

All contract deliverables shall be delivered to WSF and FTA/TRI-10 for inspection by the government technical coordinator and acceptance by the Contracting Officer's Representative (COR).

11.2   Third Party Final Inspection

WSF proposes to select a third-party inspector to be able to pick the third party evaluator, see FTA Circular 6100.1C section 6 (b) (9) (2), which is on pg III-13. The consultant, Mobilisa, and WSF personnel will assist, as necessary, the third-party evaluator.

12.0 Cost Proposal

12.1 Overall Budget by Category

	CY 2003	CY 2004	Total
WSF Personnel	$32,040	$36,160	**$68,200**
Consultant (Mobilisa)	$294,000	$325,484	**$619,484**
Material & Equipment	$52,000	$172,985	**$224,985**
Outside Evaluation		$55,000	**$55,000**
			$967,669

12.2 Overall Budget by Task

	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6	Total
WSF Personnel	$3,400	$1,000	$15,000	$21,000	$2,400	$25,400	$68,200
Consultant (Mobilisa)	$40,000	$35,000	$99,600	$220,000	$1,500	$223,384	$619,484
Material & Equipment	$2,500	$2,500	$40,000	$129,985	$0	$50,000	$224,985
Outside Evaluation	$0	$0	$0	$0	$55,000	$0	$55,000
Per Task	**$45,900**	**$38,500**	**$154,600**	**$370,985**	**$58,900**	**$298,784**	
Running Total		$84,400	$239,000	$609,985	$668,885	$967,669	

12.3 Determination of Costs

Please note that the costs are estimated given the nature of the research and development project. Equipment costs are not known given the wide range of prices for varying equipment. Some omni-direction antenna cost approximately $150, and planar array antennas cost in the vicinity of $14,000 a piece. The backhaul experimentation and site surveys will determine the equipment requirements.

12.4 Labor Categories and Rates

WSF and Mobilisa Labor Categories and Labor Rates are attached in a separate document.

Mobilisa accounting system and labor rates are review annually by the Defense Contracting Audit Agency (DCAA). Their most recent successful DCAA audit was 30 April 2003.